

①9 RÉPUBLIQUE FRANÇAISE  
INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE  
PARIS

①1 N° de publication :  
(à n'utiliser que pour les  
commandes de reproduction)

2 773 405

②1 N° d'enregistrement national :

98 00125

⑤1 Int Cl<sup>6</sup> : G 07 C 1/32 // G 06 F 12/14

⑫

## DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 08.01.98.

③0 Priorité :

④3 Date de mise à la disposition du public de la  
demande : 09.07.99 Bulletin 99/27.

⑤6 Liste des documents cités dans le rapport de  
recherche préliminaire : *Se reporter à la fin du  
présent fascicule*

⑥0 Références à d'autres documents nationaux  
apparentés :

⑦1 Demandeur(s) : FRANCE TELECOM Societe ano-  
nyme — FR.

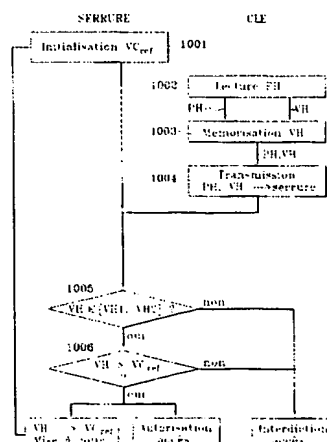
⑦2 Inventeur(s) : CLERC FABRICE et GIRAULT MARC.

⑦3 Titulaire(s) :

⑦4 Mandataire(s) : CABINET PLASSERAUD.

⑤4 PROCÉDE ET SYSTÈME DE CONTRÔLE D'ACCÈS A UNE RESSOURCE LIMITE A CERTAINES PLAGES  
HORAIRES.

⑤7 Pour contrôler l'accès d'une clé électronique à une  
serrure électronique, à l'intérieur d'une plage horaire  
prédéterminée: on initialise la serrure par une valeur de  
comptage de référence; puis, lors de chaque tentative d'ac-  
cès de la clé à la serrure: dans la clé, on lit une plage horaire  
préalablement mémorisée; on mémorise une valeur horaire  
courante délivrée par une horloge temps réel; on transmet  
de la clé à la serrure la plage horaire et la valeur horaire cou-  
rante; et, dans la serrure: on vérifie la cohérence de la va-  
leur horaire courante avec la plage horaire, et avec la valeur  
de comptage de référence; s'il y a cohérence, on autorise  
l'accès, et on met à jour la valeur de comptage de référence,  
à partir de la valeur horaire courante transmise; sinon, on in-  
terdit l'accès de la clé à la serrure.



FR 2 773 405 - A1



**PROCÉDÉ ET SYSTÈME DE CONTRÔLE D'ACCÈS À UNE RESSOURCE  
LIMITÉ À CERTAINES PLAGES HORAIRES**

La présente invention concerne un procédé et un système  
5 de contrôle d'accès à une ressource limité à certaines  
plages horaires.

Elle s'applique au contrôle d'accès à une ressource  
quelconque, ressource accédée, dont on souhaite contrôler  
l'utilisation, et dont on souhaite limiter l'accès à une ou  
10 plusieurs plages horaires déterminées, dites aussi plages de  
validité prédéterminées, que la ressource considérée soit un  
bâtiment, un système informatique, ou tout autre objet, tel  
qu'une boîte aux lettres ou un coffre de banque.

L'invention s'applique plus particulièrement au  
15 contrôle d'accès à des ressources accédées non autonomes en  
énergie et/ou ne disposant que d'un potentiel limité de  
vérification d'une plage horaire de validité, notamment les  
ressources ne disposant pas d'horloge temps réel.

La plage de validité peut être, soit la période  
20 proprement dite pendant laquelle il est possible d'accéder à  
la ressource, soit tout autre paramètre permettant de  
limiter dans le temps une attaque par utilisation  
frauduleuse de la ressource accédante.

Le principal avantage d'un moyen d'accès logique à une  
25 ressource par rapport à un moyen d'accès physique réside  
généralement dans la possibilité de ne permettre l'accès à  
la ressource qu'à l'intérieur d'une plage horaire  
relativement courte prédéterminée.

Dans ces conditions, si la clé électronique est perdue,  
30 volée, cédée ou dupliquée, elle ne permettra pas à son  
détenteur illégitime d'accéder à la ressource en dehors de  
la plage horaire prédéterminée. Cela suppose cependant que

la ressource accédée soit en mesure de vérifier que cette plage horaire est respectée. Cela implique généralement que la ressource accédée dispose d'une horloge temps réel.

Ainsi, le document FR-A-2 722 596 décrit un système de  
5 contrôle d'accès limités à des plages horaires autorisées et renouvelables au moyen d'un support de mémorisation portable. Ce système, fondé sur des mécanismes cryptographiques, permet de limiter la période de validité des droits d'accès à une courte durée, afin d'éviter une  
10 utilisation illégitime en cas de perte, vol, cession ou duplication illicite.

Toutefois, la solution décrite repose sur l'hypothèse, fortement contraignante, que la ressource accédée soit autonome en énergie, pour maintenir une horloge temps réel  
15 lui permettant de vérifier la validité de la plage horaire dans laquelle a lieu la tentative d'accès par la ressource accédante.

La présente invention a pour but de remédier aux inconvénients précités en permettant à la ressource accédée  
20 de vérifier la plage de validité sans pour autant disposer d'une horloge temps réel.

Dans ce but, la présente invention propose un procédé de contrôle d'accès d'au moins une clé électronique, munie d'une horloge temps réel délivrant une valeur horaire  
25 courante, à au moins une serrure électronique, à l'intérieur d'une plage horaire prédéterminée, remarquable en ce que :

(a) on initialise la serrure électronique par une valeur de comptage de référence ;

puis, lors de chaque tentative d'accès de la clé  
30 électronique à une serrure électronique :

dans la clé électronique :

(b) on lit une plage horaire prédéterminée, préalablement mémorisée dans la clé électronique ;

(c) on mémorise une valeur horaire courante délivrée par l'horloge temps réel ;

5 (d) on transmet de la clé électronique à la serrure électronique la plage horaire et la valeur horaire courante, et

dans la serrure électronique :

10 (e) on vérifie que la valeur horaire courante transmise est à l'intérieur de la plage horaire prédéterminée, et qu'elle est postérieure à la valeur de comptage de référence mémorisée dans la serrure ;

(f) si les vérifications effectuées à l'étape (e) sont satisfaites, on autorise l'accès, et on met à jour la valeur  
15 de comptage de référence, à partir de la valeur horaire courante transmise ;

(g) si la valeur horaire courante transmise est à l'extérieur de la plage horaire prédéterminée, ou si elle est antérieure à la valeur de comptage de référence  
20 mémorisée dans la serrure, on interdit l'accès de cette clé à cette serrure.

Dans un mode de réalisation qui procure une sécurité accrue, on effectue les étapes supplémentaires ci-après.

Dans la clé électronique :

25 (b1) à l'étape (b), on lit, en plus de la plage horaire, ou en lieu et place de la plage horaire, une signature électronique de la plage horaire, préalablement calculée et mémorisée dans la clé électronique ;

(d1) à l'étape (d), on transmet de la clé électronique  
30 à la serrure électronique, en plus de la plage horaire, ou en lieu et place de la plage horaire et de la valeur horaire courante, la signature et la valeur horaire courante, et

dans la serrure électronique :

(e1) avant l'étape (e), on vérifie la signature transmise, à partir d'une clé de vérification spécifique ;

5 (f1) à l'étape (f), on n'autorise l'accès, et on ne met à jour la valeur de comptage de référence, à partir de la valeur horaire courante transmise, que si les vérifications effectuées aux étapes (e1) et (e) sont satisfaites ;

10 (g1) à l'étape (g), on interdit l'accès de cette clé à cette serrure si la valeur horaire courante transmise est à l'extérieur de la plage horaire, ou si elle est antérieure à la valeur de comptage de référence mémorisée dans la serrure, ou si la vérification effectuée à l'étape (e1) n'est pas satisfaite.

15 En variante, l'ordre d'exécution des étapes (e1) et (e) peut être interverti.

La clé de vérification spécifique utilisée à l'étape (e1) peut être une clé publique ou secrète.

La plage horaire précitée peut comprendre plusieurs plages horaires disjointes.

20 Dans un mode particulier de réalisation, la plage horaire est un intervalle comportant deux bornes exprimées chacune comme une date en jour, mois, année et un horaire en heures, minutes, secondes.

25 La présente invention propose également un système de contrôle d'accès électronique, à l'intérieur d'une plage horaire prédéterminée, comportant au moins une serrure électronique et au moins une clé électronique, remarquable en ce que la clé comprend

30 - une horloge temps réel délivrant une valeur horaire courante, et

- un module de transmission à la serrure d'une plage horaire prédéterminée, et en ce que la serrure comprend

- un module de mémorisation accessible en lecture et en écriture,

5       - un module de comptage, ce module de comptage étant mis à jour à partir de la valeur horaire courante à chaque tentative d'accès réussie, et

10       - un module de comparaison de la valeur horaire courante à la plage horaire prédéterminée et à la valeur mémorisée dans le module de comptage.

Dans un mode de réalisation qui procure une sécurité accrue, le module de transmission à la serrure d'une plage horaire prédéterminée s'accompagne d'un module de transmission à la serrure d'une signature électronique de la  
15   plage horaire, et la serrure comprend en outre un module de vérification de la signature électronique transmise par la clé.

Dans un mode particulier de réalisation, le module de mémorisation comprend une mémoire non volatile  
20   reprogrammable électriquement.

Dans un mode particulier de réalisation, la clé électronique communique avec la serrure électronique à l'aide d'un module de transmission sans contact, par induction électromagnétique.

25       Ce module de transmission sans contact peut comprendre un premier bobinage électromagnétique prévu dans la clé et un second bobinage électromagnétique prévu dans la serrure.

Ces deux bobinages peuvent être concentriques.

D'autres caractéristiques et avantages de la présente  
30   invention apparaîtront à la lecture de la description

détaillée qui suit d'un mode particulier de réalisation, donné à titre d'exemple non limitatif.

La présente invention se réfère aux dessins annexés, dans lesquels :

- 5       - la figure 1 est un organigramme du procédé de contrôle d'accès de la présente invention, dans un mode particulier de réalisation ;
- la figure 2 est un organigramme du procédé de contrôle d'accès de la présente invention, dans un autre  
10   mode particulier de réalisation ;
- la figure 3 représente de façon schématique le système de contrôle d'accès de la présente invention, dans un mode particulier de réalisation ;
- la figure 4 représente de façon schématique le  
15   système de contrôle d'accès de la présente invention, dans un autre mode particulier de réalisation ; et
- la figure 5 représente de façon schématique le module de transmission sans contact permettant à la clé électronique de communiquer avec la serrure électronique,  
20   dans un mode particulier de réalisation.

Dans toute la suite, on considère une clé électronique utilisée pour une tentative d'accès à une serrure électronique. La clé et la serrure électroniques disposent d'une unité de calcul. La clé électronique est munie d'une  
25   horloge temps réel. Cette horloge temps réel délivre une valeur horaire courante VH, exprimée par exemple en jour, mois, année, heures, minutes, secondes. On souhaite limiter l'accès de la clé à la serrure à une plage horaire donnée PH, définie comme l'intervalle de temps compris entre deux  
30   valeurs horaires VH1 et VH2 déterminées :  $PH = [VH1, VH2]$ , ou

de manière plus large comme une réunion de tels intervalles :  $PH = [VH1, VH2] \cup [VH3, VH4] \cup \dots \cup [VHn-1, VHn]$ .

Comme l'indique la figure 1, une première étape 1001 du procédé consiste à initialiser la serrure électronique par  
5 une valeur de comptage de référence  $VC_{ref}$ .

On considère ensuite une situation où la clé électronique tente d'accéder à la serrure électronique. Cette situation peut se traduire de diverses façons, selon la forme et la nature des supports contenant la clé et la  
10 serrure. A titre d'exemple non limitatif, si la clé comporte une partie tubulaire ou en forme de languette plate, la tentative d'accès se fait par introduction de la partie tubulaire dans une cavité tubulaire complémentaire de la serrure, ou dans une fente complémentaire, respectivement.

15 Un protocole de vérification du droit d'accès de cette clé à cette serrure est alors mis en œuvre successivement dans la clé et dans la serrure.

Dans la clé, comme indiqué en 1002 sur la figure 1, on lit une plage horaire prédéterminée PH, qui a été  
20 préalablement mémorisée dans la clé électronique.

Comme indiqué en 1003, lors de la tentative d'accès, on mémorise dans la clé la valeur horaire courante VH délivrée par l'horloge temps réel de la clé.

Puis on transmet, en 1004, la plage de validité ainsi  
25 que la valeur horaire courante VH à la serrure.

Les étapes suivantes de vérification ont alors lieu dans la serrure.

En 1005 et 1006, on vérifie, d'une part, la cohérence entre la valeur horaire courante transmise VH et la plage  
30 horaire prédéterminée PH, et d'autre part, la cohérence



entre VH et la valeur de comptage de référence  $VC_{ref}$  mémorisée dans la serrure.

Par exemple, dans le cas d'une plage horaire réduite à un intervalle  $[VH1, VH2]$ , on vérifie que VH est postérieure à  
5 VH1 et antérieure à VH2, et que VH est postérieure à  $VC_{ref}$ .

Si l'une des vérifications effectuées aux étapes 1005 et 1006 donne lieu à une réponse négative, on interdit l'accès de cette clé à cette serrure.

Si l'ensemble de ces vérifications a été satisfait, on  
10 autorise l'accès, et on met à jour  $VC_{ref}$  en la remplaçant par exemple par la valeur horaire courante VH.

On décrit ci-après un autre mode de réalisation du procédé de l'invention, qui procure une sécurité accrue par rapport au mode de réalisation précédent.

15 On considère une ressource accédée non autonome en énergie et/ou ne disposant que d'un potentiel limité de vérification d'un droit d'accès.

Par « droit d'accès », on entend la signature électronique d'une plage de validité. Une signature  
20 électronique peut être obtenue à l'aide de mécanismes cryptographiques divers, tels que des mécanismes de chiffrement, ou d'authentification. Elle peut par exemple être obtenue à l'aide d'un algorithme de signature à clé secrète ou d'un algorithme de signature à clé publique.

25 Lorsqu'une « ressource accédante », ou « clé électronique », présente un droit d'accès à une « ressource accédée », ou « serrure électronique », un protocole de vérification du droit d'accès est mis en œuvre. Dans ce mode de réalisation, ce protocole comporte, en plus de la  
30 vérification de la plage de validité, la vérification de la signature électronique de cette plage de validité.

Dans ce mode de réalisation, la plage de validité peut être, soit la période proprement dite pendant laquelle il est possible d'accéder à la ressource, soit la période de validité d'une clé de signature de la ressource accédante  
5 lui permettant de s'authentifier vis-à-vis de la ressource accédée, soit tout autre paramètre permettant de limiter dans le temps une attaque par utilisation frauduleuse de la ressource accédante.

Comme l'indique la figure 2, dans ce mode de  
10 réalisation, une première étape 2001 consiste, de même qu'à l'étape 1001 dans le mode de réalisation précédent, à initialiser la serrure électronique par une valeur de comptage de référence  $VC_{ref}$ .

Dans le cas où la signature électronique S utilisée est  
15 calculée à l'aide d'un algorithme à clé publique, du type RSA (Rivest Shamir Adleman) par exemple, on mémorise dans la serrure électronique la clé publique  $K_p$  de vérification de la signature.

La signature électronique S peut également être  
20 calculée à l'aide d'un algorithme à clé secrète, du type DES (Data Encryption Standard) par exemple. Dans ce cas, contrairement au cas précédent, la clé de vérification qui est mémorisée dans la serrure à l'étape 2001 est secrète. De ce fait, elle devra être stockée dans une mémoire  
25 physiquement protégée, de sorte qu'elle ne puisse être ni lue, ni modifiée par une entité non autorisée.

On considère ensuite une situation où la clé électronique tente d'accéder à la serrure électronique. De même que dans le mode de réalisation précédent, un protocole  
30 de vérification du droit d'accès de cette clé à cette serrure est mis en œuvre successivement dans la clé et dans la serrure.

Dans la clé, comme indiqué en 2002 sur la figure 2, on lit ou on établit une signature électronique  $S(PH)$  de la plage horaire prédéterminée  $PH$ . Cette étape a lieu, soit en plus, soit en lieu et place de l'étape 1002 de lecture de la  
5 plage horaire  $PH$  du mode de réalisation précédent.

Cette signature électronique  $S(PH)$  peut avoir été calculée au préalable, par exemple par une entité extérieure de calcul de signatures, indépendante de la clé.

Dans ce cas, lors d'une étape de chargement, par  
10 exemple au moyen d'une borne de validation, une entité de validation transfère et mémorise la signature  $S(PH)$  dans la clé avant que cette clé soit mise en service.

En variante, la clé peut établir elle-même la signature, si on a mémorisé dans la clé électronique la clé  
15 privée nécessaire à cette opération, ainsi que l'algorithme cryptographique de signature, et si cette clé dispose des ressources calculatoires nécessaires.

Comme indiqué en 2003, lors de la tentative d'accès, on mémorise dans la clé la valeur horaire courante  $VH$  délivrée  
20 par l'horloge temps réel de la clé.

Puis on transmet, en 2004, la signature électronique  $S(PH)$  de la plage de validité ainsi que la valeur horaire courante  $VH$  à la serrure. Si, à l'étape 2002, on a lu la plage horaire  $PH$  en plus de la signature  $S(PH)$ , on transmet  
25 également cette plage horaire  $PH$  à la serrure à l'étape 2004.

Les étapes suivantes de vérification ont alors lieu dans la serrure.

En 2005, on vérifie la signature transmise. Si  
30 l'algorithme de calcul de signatures est un algorithme à clé publique, l'étape 2005 consiste, pour la serrure électronique, à appliquer la clé publique  $K_p$ , préalablement

mémorisée dans la serrure, à l'algorithme de vérification. La vérification positive de la signature permet d'assurer l'authenticité de la plage de validité [VH1,VH2], ladite plage étant obtenue, soit par rétablissement du message au cours de l'étape de vérification de signature, soit par simple lecture si elle a été transmise en clair avec la signature.

En 2006 et 2007, on vérifie, d'une part, la cohérence entre la valeur horaire courante transmise VH et la plage horaire prédéterminée PH, et d'autre part, la cohérence entre VH et la valeur de comptage de référence  $VC_{ref}$  mémorisée dans la serrure.

Par exemple, dans le cas d'une plage horaire réduite à un intervalle [VH1,VH2], on vérifie que VH est postérieure à VH1 et antérieure à VH2, et que VH est postérieure à  $VC_{ref}$ .

Si l'une des vérifications effectuées aux étapes 2005, 2006 et 2007 donne lieu à une réponse négative, on interdit l'accès de cette clé à cette serrure.

Si l'ensemble de ces vérifications a été satisfait, on autorise l'accès, et on met à jour  $VC_{ref}$  en la remplaçant par exemple par la valeur horaire courante VH.

Un mode particulier de réalisation du système de contrôle d'accès conforme à la présente invention va maintenant être décrit à l'aide de la figure 3.

Le système comprend une clé électronique 1 et une serrure électronique 2.

La clé électronique 1 comprend un module 11 d'alimentation en énergie, du type pile ou batterie par exemple. Le module 11 alimente une horloge temps réel interne 12 qui délivre une valeur horaire courante VH telle que définie précédemment. La clé 1 comprend également une

mémoire 13, dans laquelle est mémorisée la plage de validité PH.

L'horloge temps réel 12 et la mémoire 13 sont reliées à un module 14 de communication de la clé avec la serrure. Le  
5 module 14 permet à la clé, lors de chaque tentative d'accès, de transmettre à un module 21 de communication compris dans la serrure 2 la plage horaire PH mémorisée dans la mémoire 13, ainsi que la valeur horaire courante VH délivrée par l'horloge 12.

10 Le module 21 de communication de la serrure avec la clé est relié à une mémoire 22 accessible en lecture et en écriture. La mémoire 22 comprend un module 23 de comptage, dans lequel est mémorisée une valeur de comptage de référence  $VC_{ref}$ , initialisée avant la mise en service de la  
15 serrure électronique et remise à jour à l'aide de la valeur horaire courante VH transmise par la clé 1, à chaque tentative d'accès réussie. La mémoire 22 est par exemple une mémoire reprogrammable électriquement du type EPROM ou EEPROM.

20 La serrure 2 comprend en outre un module 25 de comparaison, qui reçoit la valeur horaire courante VH transmise par la clé 1, et la compare à la plage horaire prédéfinie  $PH = [VH1, VH2]$  et à la valeur de comptage de référence  $VC_{ref}$  mémorisée dans le module 23 de comptage. Le  
25 module 25 de comparaison teste si  $VH > VH1$  et  $VH < VH2$ , et si  $VH > VC_{ref}$ .

Le module 11 d'alimentation en énergie de la clé 1 fournit éventuellement à la serrure 2 l'énergie nécessaire aux opérations de vérification effectuées par le module 25  
30 de comparaison, ainsi que l'énergie nécessaire à l'opération de remise à jour du module 23 de comptage en cas de tentative d'accès réussie.

On décrit ci-après, à l'aide de la figure 4, un autre mode de réalisation du système de contrôle d'accès de l'invention, comprenant une clé électronique 41 et une serrure électronique 42, qui procure une sécurité accrue par rapport au mode de réalisation de la figure 3.

Les éléments de ce système qui sont analogues à ceux du mode de réalisation de la figure 3 portent les mêmes chiffres de référence, et ne seront pas décrits une nouvelle fois.

10 Dans ce mode de réalisation, la mémoire 13 de la clé 41 contient non seulement la plage de validité PH, mais aussi la signature électronique S(PH) de cette plage de validité.

La module 14 de communication de la clé avec la serrure permet à la clé 41, lors de chaque tentative d'accès, de transmettre au module 21 de communication compris dans la serrure 42, non seulement la valeur horaire courante VH délivrée par l'horloge 12 et la plage horaire PH mémorisée dans la mémoire 13, mais aussi la signature électronique S(PH) mémorisée dans la mémoire 13.

20 La serrure 42 comprend, en plus du module 21 de communication avec la clé, de la mémoire 22 comprenant le module 23 de comptage, et du module 25 de comparaison, décrits précédemment, un module 24 de vérification de signature.

25 Le module 24 est relié au module 21 de communication de la serrure avec la clé et au module 25 de comparaison. Le module 24 reçoit la signature S(PH) de la plage de validité et, dans le cas où l'algorithme de calcul de signatures utilisé est un algorithme à clé publique, vérifie la signature S(PH) reçue au moyen de la clé publique  $K_p$ .

30 Le module 11 d'alimentation en énergie de la clé 41 fournit éventuellement à la serrure 42 l'énergie nécessaire

aux opérations de vérification effectuées par le module 24 de vérification de signature et le module 25 de comparaison, ainsi que l'énergie nécessaire à l'opération de remise à jour du module 23 de comptage en cas de tentative d'accès réussie.

La figure 5 illustre une réalisation matérielle particulière des modules 14 et 21 de communication entre la clé et la serrure, applicable aussi bien au mode de réalisation de la figure 3 qu'au mode de réalisation de la figure 4.

La clé 1 (ou 41 dans le cas du mode de réalisation de la figure 4) comprend une tige 30 en matière ferromagnétique, garnie d'enroulements en cuivre 31 formant un premier bobinage. Ce premier bobinage est relié au module 14 de communication de la clé avec la serrure.

A chaque tentative d'accès, la clé 1 ou 41 vient se loger dans une cavité tubulaire 32 de diamètre légèrement supérieur au diamètre de la tige 30. La cavité 32 est également garnie d'enroulements en cuivre 33 formant un second bobinage, relié au module 21 de communication de la serrure avec la clé. Les deux bobinages 31, 33 sont alors concentriques, et l'information est transmise sous forme codée binaire entre la clé et la serrure 2 (ou 42 dans le cas du mode de réalisation de la figure 4) par induction électromagnétique.

La présente invention trouve une application particulièrement adaptée à l'accès, par les préposés au courrier, à des boîtes aux lettres, qui ne sont pas autonomes en énergie.

On peut renforcer encore davantage la sécurité du contrôle d'accès, en ajoutant d'autres données aux informations de signature et de plage horaire transmises par

la clé à la serrure. Par exemple, on peut ajouter un numéro de série identifiant la clé électronique. Dans ce cas, on munit la serrure d'un module de comptage supplémentaire, associé à ce numéro de série ; on mémorise dans le module de  
5 comptage supplémentaire le début de la prochaine plage horaire au cours de laquelle une clé portant ce numéro de série pourra accéder à la serrure.



**REVENDICATIONS**

1. Procédé de contrôle d'accès d'au moins une clé électronique, munie d'une horloge temps réel délivrant une  
5 valeur horaire courante, à au moins une serrure électronique, à l'intérieur d'une plage horaire prédéterminée, caractérisé en ce que :

(a) on initialise la serrure électronique par une valeur de comptage de référence ;

10 puis, lors de chaque tentative d'accès de la clé électronique à une serrure électronique :

dans la clé électronique :

(b) on lit une plage horaire prédéterminée, préalablement mémorisée dans la clé électronique ;

15 (c) on mémorise une valeur horaire courante délivrée par l'horloge temps réel ;

(d) on transmet de la clé électronique à la serrure électronique la plage horaire et la valeur horaire courante, et

20 dans la serrure électronique :

(e) on vérifie que la valeur horaire courante transmise est à l'intérieur de la plage horaire prédéterminée, et qu'elle est postérieure à la valeur de comptage de référence mémorisée dans la serrure ;

25 (f) si les vérifications effectuées à l'étape (e) sont satisfaites, on autorise l'accès, et on met à jour la valeur de comptage de référence, à partir de la valeur horaire courante transmise ;

(g) si la valeur horaire courante transmise est à  
30 l'extérieur de la plage horaire prédéterminée, ou si elle est antérieure à la valeur de comptage de référence

mémorisée dans la serrure, on interdit l'accès de cette clé à cette serrure.

2. Procédé selon la revendication 1, caractérisé en ce que :

5 dans la clé électronique :

(b1) à l'étape (b), on lit, en plus de la plage horaire, ou en lieu et place de la plage horaire, une signature électronique de ladite plage horaire, préalablement calculée et mémorisée dans la clé  
10 électronique ;

(d1) à l'étape (d), on transmet de la clé électronique à la serrure électronique, en plus de la plage horaire, ou en lieu et place de la plage horaire et de la valeur horaire courante, ladite signature et la valeur horaire courante, et  
15 dans la serrure électronique :

(e1) avant l'étape (e), on vérifie la signature transmise, à partir d'une clé de vérification spécifique ;

(f1) à l'étape (f), on n'autorise l'accès, et on ne met à jour la valeur de comptage de référence, à partir de la  
20 valeur horaire courante transmise, que si les vérifications effectuées aux étapes (e1) et (e) sont satisfaites ;

(g1) à l'étape (g), on interdit l'accès de ladite clé à ladite serrure si la valeur horaire courante transmise est à l'extérieur de ladite plage horaire, ou si elle est  
25 antérieure à la valeur de comptage de référence mémorisée dans la serrure, ou si la vérification effectuée à l'étape (e1) n'est pas satisfaite.

3. Procédé selon la revendication 2, caractérisé en ce que l'ordre d'exécution des étapes (e1) et (e) est  
30 interverti.

4. Procédé selon la revendication 2 ou 3, caractérisé en ce que ladite clé de vérification spécifique est une clé publique ou secrète.

5 5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite plage horaire prédéterminée comprend plusieurs plages horaires disjointes.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que chaque plage horaire est un intervalle comportant deux bornes exprimées chacune comme  
10 une date en jour, mois, année et un horaire en heures, minutes, secondes.

7. Système de contrôle d'accès électronique, à l'intérieur d'une plage horaire prédéterminée, comportant au moins une serrure électronique (2;42) et au moins une clé  
15 électronique (1;41), caractérisé en ce que la clé (1;41) comprend

- une horloge temps réel (12) délivrant une valeur horaire courante (VH), et

- des moyens (14) pour transmettre à la serrure  
20 (2;42) une plage horaire (PH) prédéterminée, et en ce que la serrure (2;42) comprend

- des moyens (22) de mémorisation accessibles en lecture et en écriture,

- des moyens (23) de comptage, lesdits moyens (23)  
25 de comptage étant mis à jour à partir de ladite valeur horaire courante (VH) à chaque tentative d'accès réussie, et

- des moyens (25) de comparaison de la valeur horaire courante (VH) à la plage horaire (PH) prédéterminée et à la valeur ( $VC_{ref}$ ) mémorisée dans lesdits moyens (23) de  
30 comptage..

8. Système selon la revendication 7, caractérisé en ce que

- lesdits moyens (14) de la clé électronique (1;41) comprennent en outre des moyens pour transmettre à la serrure (2;42) une signature électronique (S(PH)) de ladite  
5 plage horaire (PH), et en ce que

- la serrure (2;42) comprend en outre des moyens (24) pour vérifier ladite signature électronique (S(PH)) transmise par la clé (1;41).

10 9. Système selon la revendication 7 ou 8, caractérisé en ce que lesdits moyens (22) de mémorisation comprennent une mémoire non volatile reprogrammable électriquement.

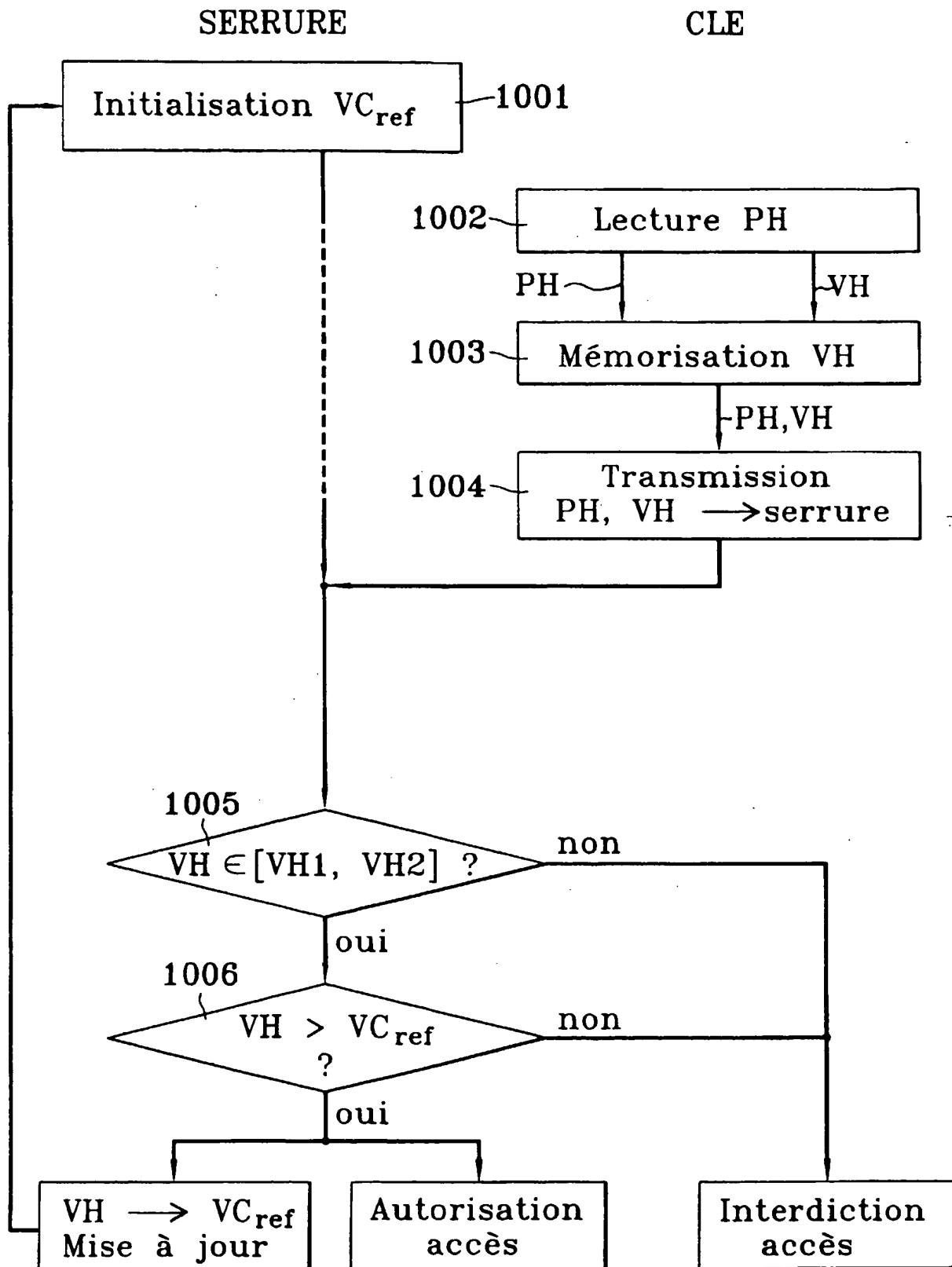
10. Système selon la revendication 7, 8 ou 9, caractérisé en ce que la clé électronique (1;41) communique  
15 avec la serrure électronique (2;42) à l'aide de moyens de transmission sans contact, par induction électromagnétique.

11. Système selon la revendication 10, caractérisé en ce que lesdits moyens de transmission sans contact comprennent un premier bobinage électromagnétique (31) prévu  
20 dans la clé (1;41) et un second bobinage électromagnétique (33) prévu dans la serrure (2;42).

12. Système selon la revendication 11, caractérisé en ce que les bobinages (31,33) prévus dans la clé (1;41) et dans la serrure (2;42) sont concentriques.

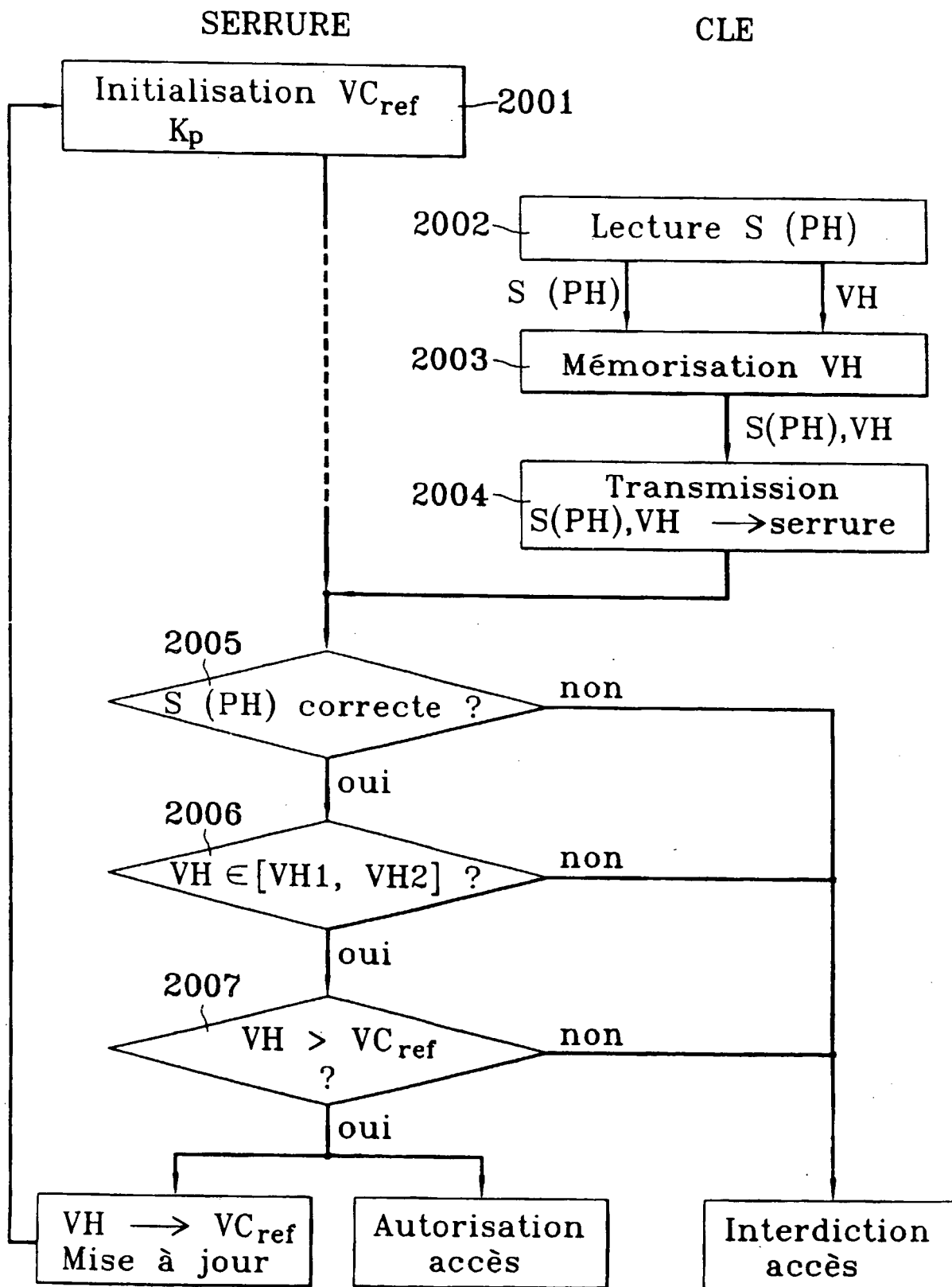
1/5

FIG. 1



2/5

FIG.2



The diagram illustrates a control system architecture, divided into two main functional blocks, 1 and 2, separated by a dashed line.

**Block 1 (Left):**

- 11 Alimentation:** Provides power to the system.
- 12 Horloge:** A clock source that provides a timing signal **VH** to block 14.
- 13 MEM:** Memory unit that provides a signal **PH** to block 14.
- 14 COMMUNICATION:** A communication interface that receives signals **VH** and **PH** and exchanges data with block 21 via a bidirectional arrow.

**Block 2 (Right):**

- 21 COMMUNICATION:** A communication interface that receives data from block 14 and sends it to block 22.
- 22:** A processing unit containing:
  - 23 MEM:** Memory unit that receives data from block 21 and provides a reference signal **VCref** to block 25.
  - 24 COMPT.:** A computation unit that receives data from block 21 and provides a signal to block 25.
- 25 COMPAR.:** A comparison unit that receives signals from block 24 and block 23, and provides a feedback signal **VH** to block 21.

4/5

FIG. 4

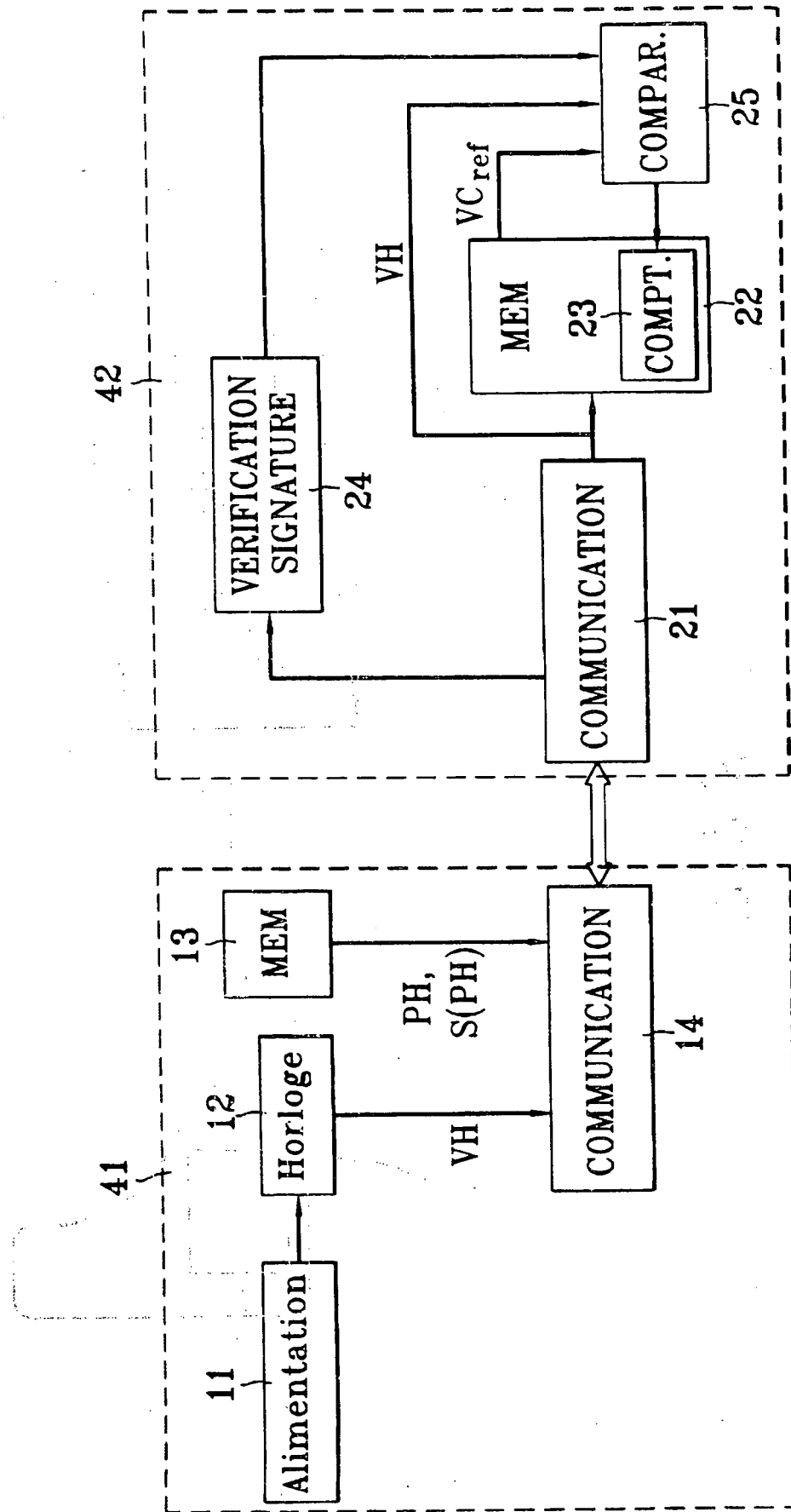




FIG. 5

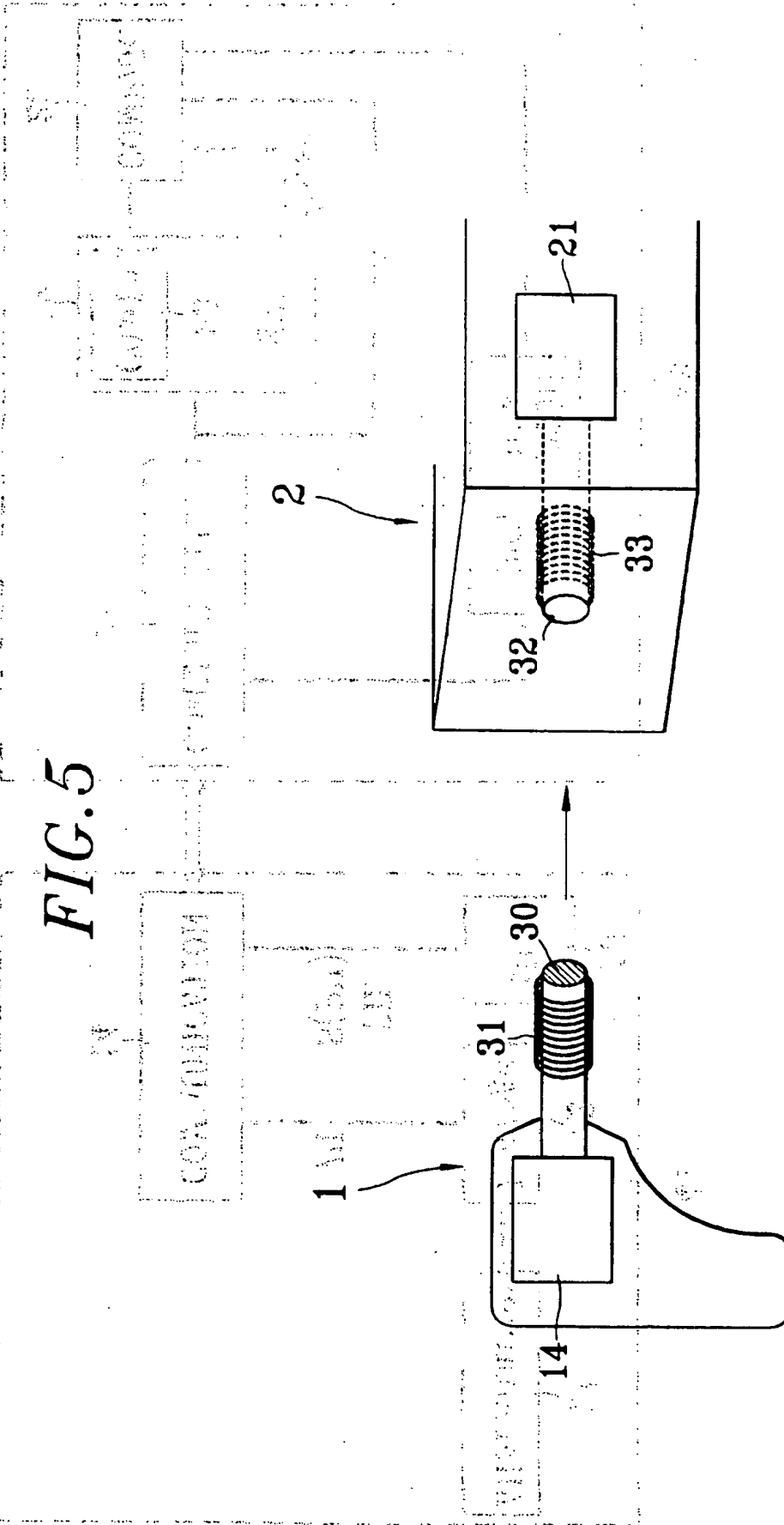


FIG. 5

INSTITUT NATIONAL

de la

PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE  
PRELIMINAIREétabli sur la base des dernières revendications  
déposées avant le commencement de la rechercheFA 554367  
FR 9800125

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	WO 93 21712 A (MEDECO SECURITY LOCKS) 28 octobre 1993 * abrégé; figures 1A, 5, 6, 8, 10 * * page 2, ligne 21 - page 3, ligne 32 * * page 5, ligne 12 - ligne 31 * * page 7, ligne 18 - page 8, ligne 8 * * page 9, ligne 1 - ligne 30 * * page 11, ligne 11 - page 12, ligne 3 * * page 17, ligne 32 - page 18, ligne 9 *	1, 7, 9
Y	EP 0 419 306 A (ROCKWELL AUTOMOTIVE BODY SYST) 27 mars 1991 * abrégé; revendications 3, 4 * * page 5, ligne 14 - ligne 20 *	1, 7, 9
A, D	FR 2 722 596 A (FRANCE TELECOM) 19 janvier 1996 * abrégé; revendications 1-3, 9, 14; figures * * page 3, ligne 6 - page 5, ligne 9 * * page 6, ligne 22 - page 7, ligne 31 * * page 11, ligne 20 - page 12, ligne 3 *	1, 2, 4-8
A	EP 0 122 244 A (WSO CPU SYSTEM AB) 17 octobre 1984 * abrégé; figures *	1, 7, 9
A	WO 82 02811 A (NELSON AVI N) 19 août 1982 * abrégé; figure 1 * * page 1, ligne 13 - page 2, ligne 34 *	10-12
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
		G07C E05B G07F
Date d'achèvement de la recherche		Examineur
9 octobre 1998		Buron, E
CATEGORIE DES DOCUMENTS CITES		
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant		

EPO FORM 1503 03 82 (P04C13)

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**